Realtime
publishers

The Shortcut Guide™ To

Subject Alternative Name Certificates

sponsored by

VeriSign®

Mike Danseglio

Introduction to Realtime Publishers

by Don Jones, Series Editor

For several years now, Realtime has produced dozens and dozens of high-quality books that just happen to be delivered in electronic format—at no cost to you, the reader. We've made this unique publishing model work through the generous support and cooperation of our sponsors, who agree to bear each book's production expenses for the benefit of our readers.

Although we've always offered our publications to you for free, don't think for a moment that quality is anything less than our top priority. My job is to make sure that our books are as good as—and in most cases better than—any printed book that would cost you $40 or more. Our electronic publishing model offers several advantages over printed books: You receive chapters literally as fast as our authors produce them (hence the "realtime" aspect of our model), and we can update chapters to reflect the latest changes in technology.

I want to point out that our books are by no means paid advertisements or white papers. We're an independent publishing company, and an important aspect of my job is to make sure that our authors are free to voice their expertise and opinions without reservation or restriction. We maintain complete editorial control of our publications, and I'm proud that we've produced so many quality books over the past years.

I want to extend an invitation to visit us at http://nexus.realtimepublishers.com, especially if you've received this publication from a friend or colleague. We have a wide variety of additional books on a range of topics, and you're sure to find something that's of interest to you—and it won't cost you a thing. We hope you'll continue to come to Realtime for your educational needs far into the future.

Until then, enjoy.

Don Jones

Copyright Statement

If you have any questions about these terms, or if you would like information about licensing materials from Realtime Publishers, please contact us via e-mail at info@realtimepublishers.com.

This sponsored eBook is valid until August 31, 2011.

Chapter 1: Introduction to Certificates

There are numerous ways to apply public key infrastructure (PKI). There are probably as many unique solutions available as there are companies to apply them to. A one-size-fits-all PKI simply does not exist. And in a similar vein, there is no perfect PKI; there is almost always a tradeoff made during the process of PKI implementation.

For example, deploying an externally managed PKI may cut costs, such as internal headcount or the deployment of intranet infrastructure servers, while incurring other costs, including monthly maintenance fees. Another, more esoteric example is key size. Many cryptographic algorithms allow an administrator to select the size of the public key used for the PKI. As you may already know, the rule is that for any cryptography, the larger you make the key, the more secure the data becomes. So many executives and IT professionals will initially decide to use the largest key possible. And if there were no downsides, that would be a great choice. However, the drawback is that intense calculations must be made every time the key is used, and particularly when the key is generated. As a result, the system becomes far more secure but far slower.

Because there is no PKI solution, you need to be familiar with as many available options as possible. This familiarity helps you determine the best way to address the stated needs. For example, let's say you need a new car. Once you've defined the intended uses (for example, commute to work, drive the kids to band practice) you can begin to identify cars that will fulfill those uses. Most people will not simply decide, "I'll buy a Ford because it's a car." They will review many brands, models, dealerships, and price points until they narrow their search. People often test drive several cars, sometimes for long enough to use the vehicle for its actual intended use. And almost invariably, the selected vehicle is a compromise. How often have you heard, "I went with the VW because even though the VW is too small, the Mazda was too expensive, and the Toyota didn't have the options I wanted." This person is making a compromise.

Selecting a PKI and approach is very much the same. You work with a broad representation of business stakeholders to identify the various business and security needs that this system will address; you then seek to meet the needs in the best possible way, as defined by your selection criteria (for example, budget, timeline, security requirements). You will most likely try out a sample implementation as a "test drive" of the PKI solution before committing to it. And then your selection will be a compromise between your driving factors. You will almost certainly have some amount of compromise in your decision because, frankly, you do not have infinite resources at your disposal.

This reality requires explanation because some readers might wonder why this guide does not provide an end-to-end usage architecture and instructions for specific use of Subject Alternative Name (SAN) certificates within a PKI. There is no way to accurately state that one solution is better than the other for a specific need without in-depth research. However, there are numerous common techniques and methods that, over time, have proven to be effective. These are the techniques that this guide will explore and recommend.

Intended Audience

A common practice for guides like this is to clearly define the intended audience. In this case, the definition is broken down by role within an IT organization. This guide is written with a few key roles in mind:

- IT generalist—IT departments are frequently small and do not allow personnel to specialize in a particular area. Every person performs tasks from multiple disciplines. These generalists work on different systems, so they need to be familiar with the basics of many technologies. This guide serves to introduce them to SAN certificates as well as provide a reference when they are performing PKI-related tasks.
- PKI specialist—This person is part of a larger IT infrastructure or a consultant who specializes in PKI and digital certificates. They do not have the broad knowledge of the generalist but instead deeply understand the mechanics and inner workings of PKI. Someone in this role can read this guide in its entirety or use pieces to meet specific needs. They can also refer other IT personnel to this guide for clarification or instruction.
- IT architect—In most organizations, an architect assesses a need and plans a solution in collaboration with many others. This person needs to be aware of virtually every possible solution to a problem in order to properly assess the problem and determine the best possible solution.

- Business Decision Maker (BDM)—There are two decision-making roles in many organizations. The first, the BDM, takes into account business drivers, budget, user and organizational needs, and IT requirements when making strategic decisions. A person in this role may, for example, decide whether to implement an internal PKI or outsource the infrastructure. This person will not, by contrast, decide to use one technology or the other. They will communicate their strategic decision and requirements to a Technical Decision Maker.
- Technical Decision Maker (TDM)—This person is complementary to the BDM. The TDM decides what specific technologies or processes are appropriate to meet the needs that are defined by the BDM and works closely with the architect to plan and the generalist and specialist to implement the plans. The TDM is often at the center of a project and, in many frameworks, is akin to the project manager.
- Hybrid—You might hold more than one of these roles or none at all. Because every IT organization is different, I cannot accurately describe 100% of the roles. As a result, this section does not define the only people who can find value in the guide. It merely explains the audience defined as part of the writing process.

How to Use This Guide

This guide is provided in four chapters. Each chapter focuses on a different aspect of the concepts and practical use of SAN certificates:

- **Chapter 1: Introduction to Subject Alternative Name Certificates**—This chapter introduces broad PKI terms that are used throughout the guide. It provides a framework for the in-depth concepts and application of SAN certificates in later chapters. Although this chapter may be considered review material for some readers, it is important to understand this information to ensure that later chapters are effective.
- **Chapter 2: SAN Certificates In Depth**—This chapter is dedicated to getting down into the details of a SAN certificate. It will examine the certificate structures and metadata and will compare data between SAN and non-SAN certificates. It will also compare SAN certificates to wildcard certificates to understand the distinction between two somewhat similar products.

- **Chapter 3: The Business Value of SAN Certificates**—Written primarily for the BDM and TDM readers, this chapter discusses the business aspect of SAN certificates. It will examine the business costs and return on investment (ROI) drivers that apply to both SAN and other similar certification strategies. This chapter supports the business and organizational elements of the solutions discussed in Chapter 2.
- **Chapter 4: Planning and Implementing a SAN-Enabled Certificate Strategy**—This chapter discuss the details of actually implementing a SAN-enabled certificate strategy. Topics include analyzing existing systems and properly planning for a SAN certificate deployment. Ongoing operations-based tasks are also explored. This chapter is useful for the implementers in an organization, such as the IT generalist or specialist, and the planning elements apply to architects as well.

What Are Certificates?

In the past, a certificate has been an official document asserting facts in a trustworthy manner. For many of us, the first example we encounter is our birth certificate. It contains information such as our date of birth and name. It is signed and usually stamped by the issuing authority, usually by the hospital or local government. Later in life, we can use this certificate to assert our identity when we enroll in school or secure a loan.

Modern certificates are much the same. They assert some detailed information in a trustworthy manner, vouched for by an issuing authority. But nowadays, certificates convey different detailed data.

> Within the context of this guide, consider the term “certificates” to be digital certificates unless otherwise noted.

Certificates contain a great deal of data that can be used for a variety of purposes. Let’s take a closer look at the data inside the certificate and how it gets used in a variety of ways.

What Do Certificates Do?

Although you are probably already familiar with digital certificates (referred to as simply "certificates" from here on), it is worth defining them clearly. A certificate is a data structure that provides a digitally secure representation of the holder's identity. This data includes keys that make the certificate extremely difficult to modify or spoof without detection.

Certificates, by themselves, have limited use. A certificate is made up of data that provides the following information at minimum:

- Certificate holder
- Certificate issuer
- Public key
- Intended use

  This is the bare minimum information that a certificate contains. Most certificates have a great deal more information to make them useful to a wide variety of services and applications.

This information allows a computer (the certificate holder) to assert its identity in a trustworthy manner and initialize secure communication. An important distinction here is that although the certificate supports and enables a number of critical security functions including authentication and encryption, the certificate does not act on those functions. For example, a certificate is normally used when two computers establish a secure communications channel. The certificate and the associated PKI provide the data and identity support necessary to initialize that process. But the secure communication itself must be performed by a service or application designed to do so, such as the use of Secure Sockets Layer (SSL) in Internet browsers and Web servers.

Common uses of certificates include:

- Data encryption using common protection technologies such as Windows Encrypting File System (EFS)
- Email signing and encryption
- IP Security (IPSec) to establish authenticated and encrypted communication between multiple computers or isolate portions of a network
- SSL for authenticated and encrypted communication between Web servers and clients

There are many other uses that are less common. If they are central to your business operations, they may be critical. This list is just a brief sampling.

Software is readily available on the Internet for generating digital certificates. Anyone—from the US government to major corporations to a lone malware developer—can generate digital certificates. This is analogous to anyone being able to issue drivers licenses. You can imagine how much credibility a police officer would give to someone driving with a license issued from "Acme Mail Order Licenses" or some other fly-by-night outfit. The value of a digital certificate does not lie just with the certificate itself but with the credibility and reputation of the institution that issued it. In a word, it is all about trust.

What Is Trust?

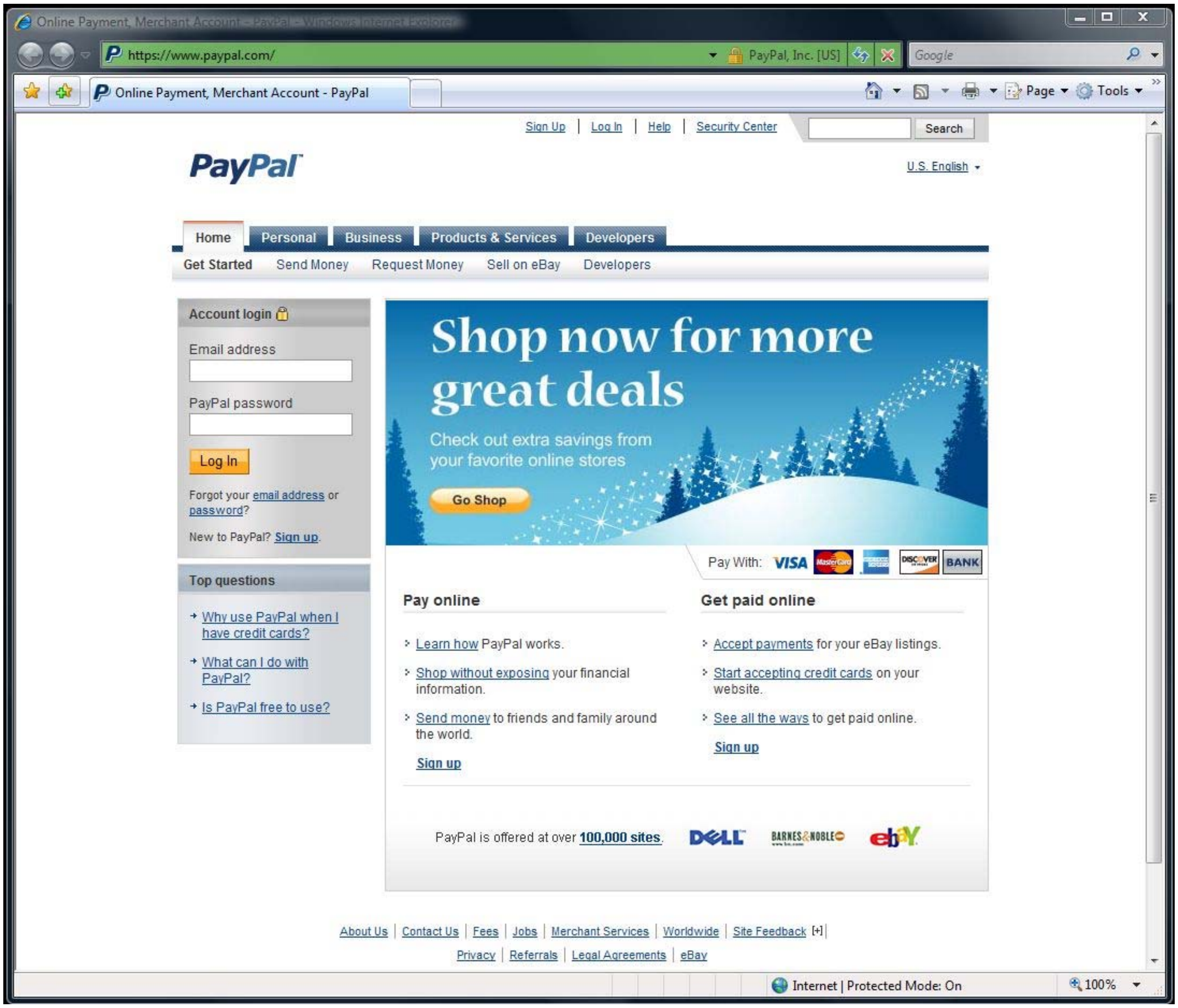
A central theme for PKI and certificates is trust. Trust is itself somewhat difficult to describe, as there are both technical and perception components that combine to form what we define as trust.

Consider your decision about which bank to use. When you were trying to select a bank, a number of factors entered your mind. Will the bank be in business for a long time? Is my money safe? Does the bank have a good reputation with other customers? Does the bank have a great deal of assets to ensure its long-term viability? These are all great questions and you probably had many more. But in the end, no matter how much research you did, you had to trust your money with your bank and trust that the bank will not go out of business or steal your money.

Now consider an example from ecommerce. Ten years ago you might not have heard of a new company called eBay and therefore would have been hesitant to do business with it. How can a startup or small company offer proof to potential customers that it is a legitimate business? After all, as Peter Steiner's famed *New Yorker* cartoon captured so well, "On the Internet, nobody knows you're a dog" (Source: http://www.unc.edu/depts/jomc/academics/dri/idog.html). What kind of due diligence can you expect when picking an online vendor? It is simply not reasonable to assess each vendor's trustworthiness. A better option is to find a business you trust that will perform the due diligence work to evaluate vendors. That's where digital certificate issuers come in.

When you examine a certificate, you can always determine what company or entity issued the certificate. The issuer trusted the certificate subject in order to actually sign and issue the certificate. Therefore, you are also trusting the subject and the issuer when you accept and use a certificate.

Let's look at a very common example. Figure 1.1 shows a Web site, PayPal, that uses certificates and SSL for authentication and communication.



Forgot your email address or password?

New to PayPal? Sign up.

- Why use PayPal when I have credit cards?
- What can I do with PayPal?
- Is PayPal free to use?

Shop now for more great deals

Check out extra savings from your favorite online stores

Pay online

- Learn how PayPal works.
- Shop without exposing your financial information.
- Send money to friends and family around the world.

Sign up

Get paid online

- Accept payments for your eBay listings.
- Start accepting credit cards on your website.
- See all the ways to get paid online.

Sign up

PayPal is offered at over 100,000 sites.

About Us | Contact Us | Fees | Jobs | Merchant Services | Worldwide | Site Feedback [+] |
Privacy | Referrals | Legal Agreements | eBay

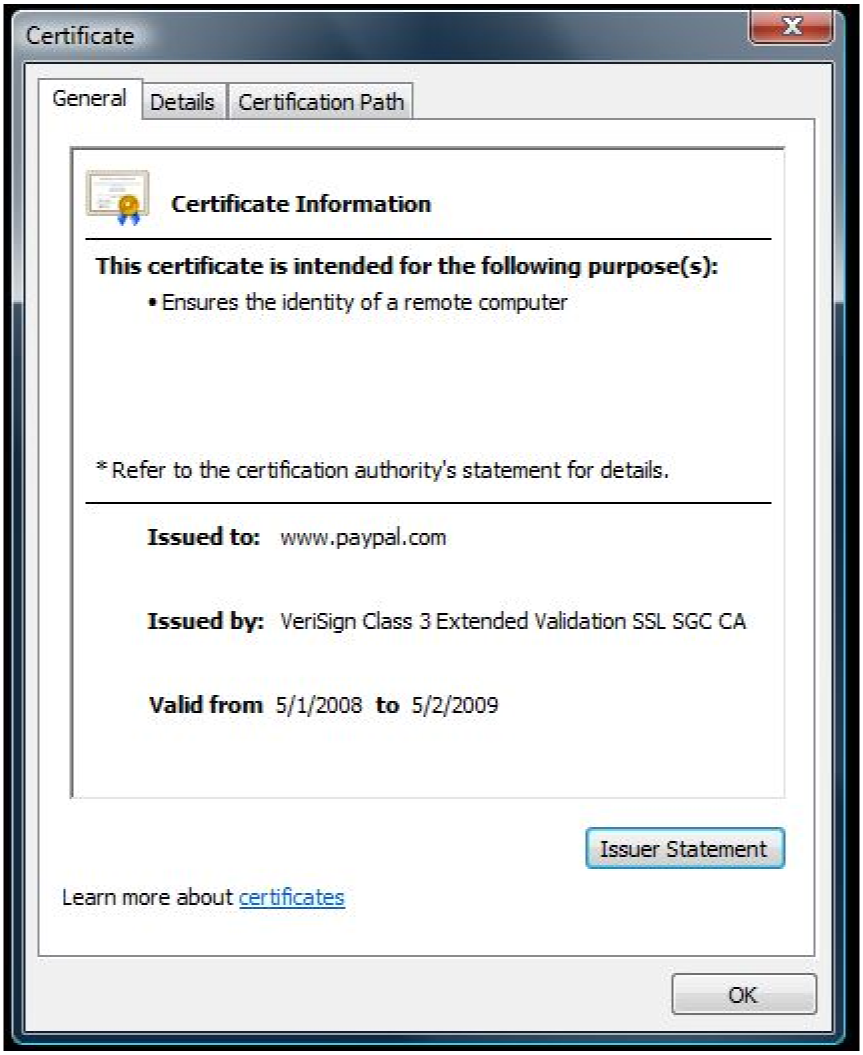
Figure 1.1: PayPal's Web site—notice the green address bar and the padlock identifying the Web site.

PayPal obviously wants the users to trust its Web site, as the company handles financial transactions and the site is linked to bank accounts. In fact, the site is using an Extended Validation (EV) SSL Certificate that suggests an additional level of trust.

Cross Reference

For more information about EV SSL Certificates, see http://nexus.realtimepublishers.com/SGEVSC.htm.

To help facilitate that trust, the Web site uses certificates that chain to a well-known root Certification Authority (CA). To show this clearly, let's look at Figures 1.2 and 1.3.



Certificate

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

* Refer to the certification authority's statement for details.

Issued to: www.paypal.com

Issued by: VeriSign Class 3 Extended Validation SSL SGC CA

Valid from 5/1/2008 to 5/2/2009

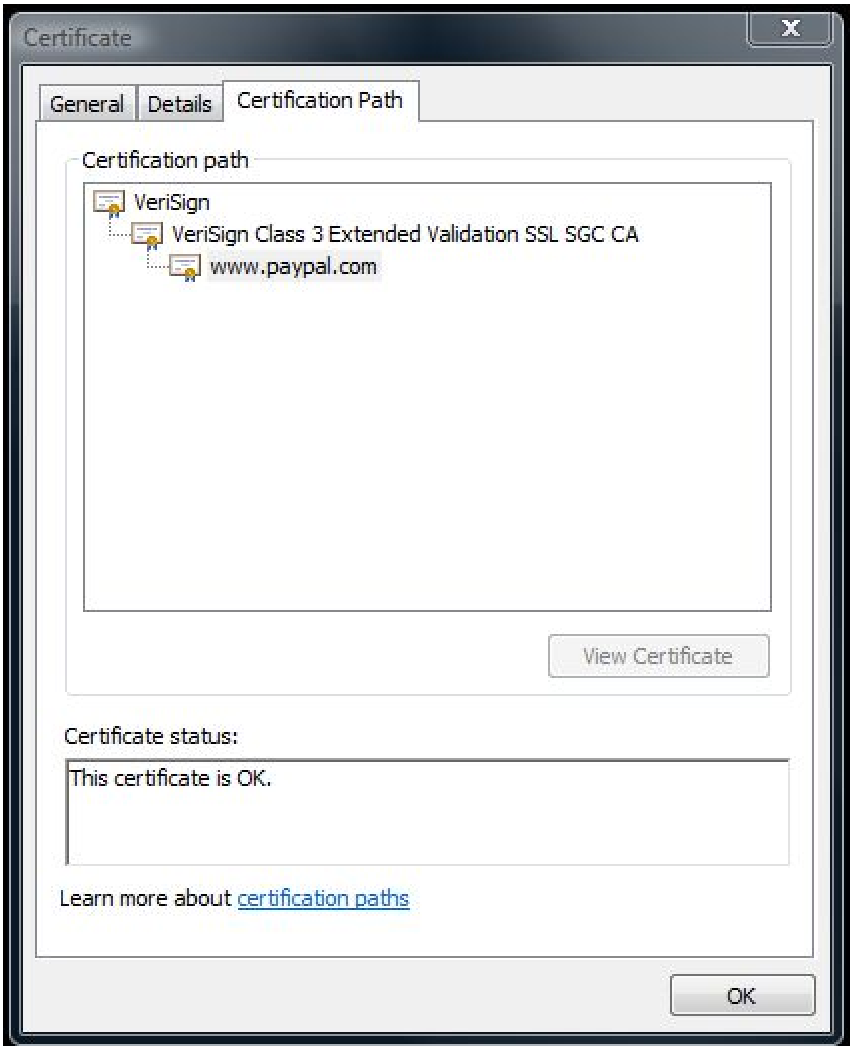
Figure 1.2: The PayPal Web site certificate showing the intended use for the certificate.

Figure 1.2 is the default certificate view in Windows. It shows a great deal of information that is often considered when a client decides whether to trust the Web site. The information on this screen is explained in Table 1.1.

Certificate Field	Description
Intended purposes	A list that describes what the certificate can be used for
Issued by	The CA that issued the certificate
Issued to	The party that requested, received, and is now using the certificate
Valid from	Date range for which the certificate is valid

Table 1.1: Basic information listed for a certificate.

When you select the Certification Path tab in this dialog box, you can examine the chain of trust. This chain includes all certificates from the one being examined to the trusted root certificate.



VeriSign
VeriSign Class 3 Extended Validation SSL SGC CA
www.paypal.com

Certificate status:

This certificate is OK.

Learn more about certification paths

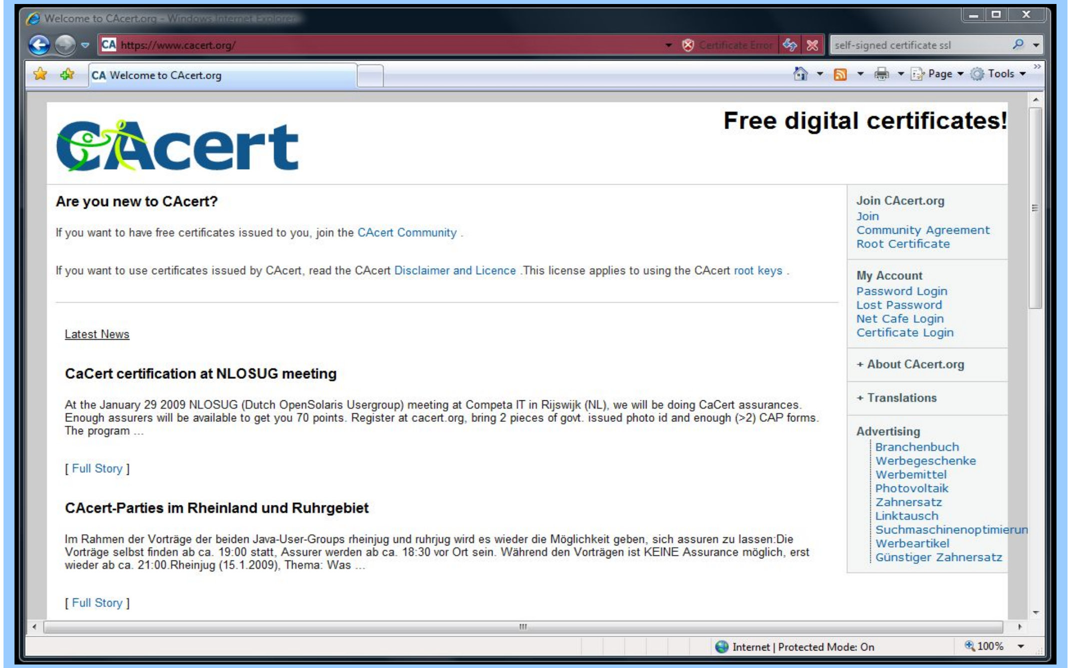
Figure 1.3: Detail of the PayPal Web site certificate showing its chain to the trusted VeriSign root certificate.

Is this information sufficient to decide whether to trust the certificate or the subject? There is no cut-and-dry answer to that question. Someone in an IT group may believe that this certificate is not trustworthy enough because of past issues with the root certificate. A client seeing this certificate in their Web browser may not be familiar with the root CA. Others might recognize the name or do research and decide that they want to trust the certificate and, by proxy, the information protected by the certificate.

Levels of Trust

Different certificates can provide different levels of trust. In a perfect world, every certificate would be entirely trustworthy. And for a while, many people in the IT field believed that. But as we've discussed, anyone can get a digital certificate, whether from a less-than-ideal public PKI or by creating his or her own PKI and issuing a certificate there (there are free PKI software packages available today for this purpose). Thus, the usefulness of a digital certificate relies entirely on whether it is trusted when presented.

For example, there are dozens of certificates—issued by recognizable companies including VeriSign, GTE, Entrust, Thawte, and Microsoft itself—built-in to and trusted by a standard Windows installation. These certificates have gone through a specific trust process with Microsoft before being included. That process provides a specific level of trustworthiness. By contrast, certificates from individual companies that offer no assurance of trustworthiness or identification are not included by default. Acme Corporation may create a PKI and issue itself a self-signed certificate that I encounter when using their ordering process. Acme may be trustworthy, but their certificate is still not trusted by default and requires me to explicitly trust it before use. Figure 1.4 offers a great example of a Web site that is using an untrusted, self-signed certificate. This page is only shown after clicking through a warning that the certificate is not trusted and should be scrutinized.



Are you new to CAcert?

If you want to have free certificates issued to you, join the CAcert Community .

If you want to use certificates issued by CAcert, read the CAcert Disclaimer and Licence .This license applies to using the CAcert root keys .

Latest News

CaCert certification at NLOSUG meeting

At the January 29 2009 NLOSUG (Dutch OpenSolaris Usergroup) meeting at Competa IT in Rijswijk (NL), we will be doing CaCert assurances. Enough assurers will be available to get you 70 points. Register at cacert.org, bring 2 pieces of govt. issued photo id and enough (>2) CAP forms. The program ...

[Full Story]

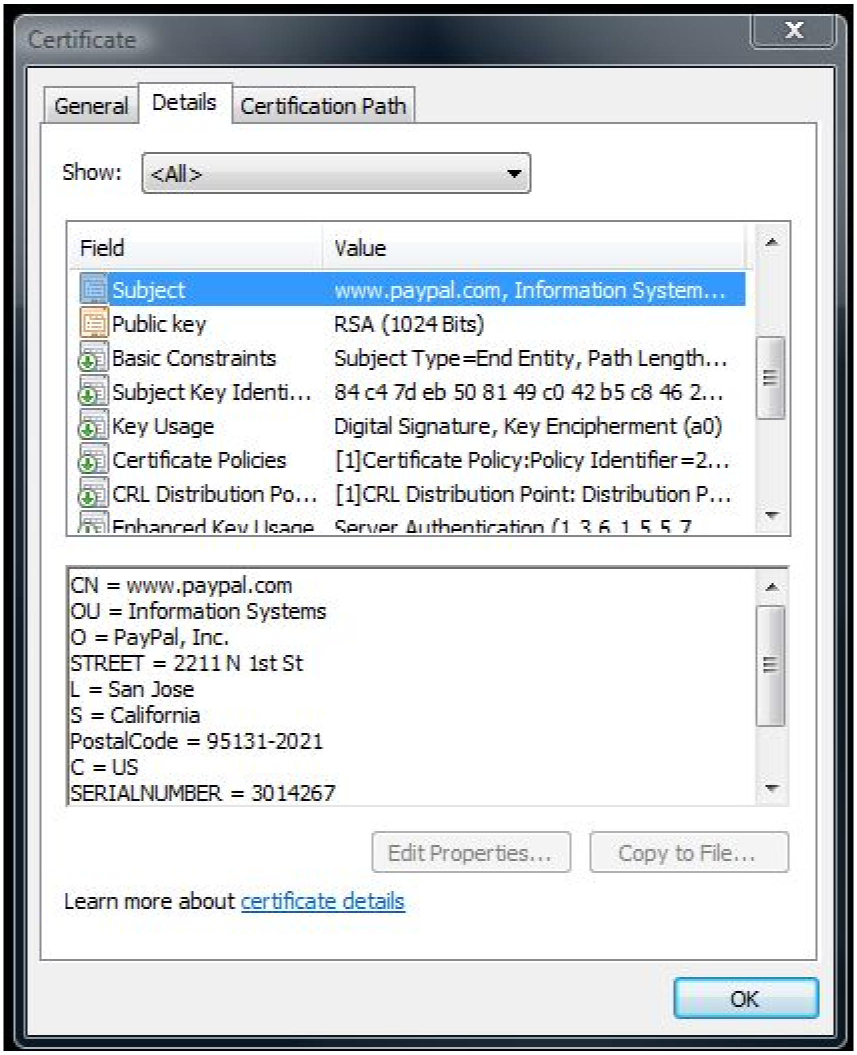
CAcert-Parties im Rheinland und Ruhrgebiet

Im Rahmen der Vorträge der beiden Java-User-Groups rheinjug und ruhrjug wird es wieder die Möglichkeit geben, sich assuren zu lassen:Die Vorträge selbst finden ab ca. 19:00 statt, Assurer werden ab ca. 18:30 vor Ort sein. Während den Vorträgen ist KEINE Assurance möglich, erst wieder ab ca. 21:00.Rheinjug (15.1.2009), Thema: Was ...

[Full Story]

Figure 1.4: A Web site using an untrusted, self-signed certificate. Notice the red address bar and red security shield.

There is another portion of the certificate that hasn't yet been illustrated. Figure 1.5 shows the Details tab of the certificate, which includes a great deal of technical information about the contents of the certificate.



Field	Value
Subject	www.paypal.com, Information System...
Public key	RSA (1024 Bits)
Basic Constraints	Subject Type=End Entity, Path Length...
Subject Key Identi...	84 c4 7d eb 50 81 49 c0 42 b5 c8 46 2...
Key Usage	Digital Signature, Key Encipherment (a0)
Certificate Policies	[1]Certificate Policy:Policy Identifier=2...
CRL Distribution Po...	[1]CRL Distribution Point: Distribution P...
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7

CN = www.paypal.com
OU = Information Systems
O = PayPal, Inc.
STREET = 2211 N 1st St
L = San Jose
S = California
PostalCode = 95131-2021
C = US
SERIALNUMBER = 3014267

Figure 1.5: The details of the certificate.

In this case, the Subject field was selected to show the details of the certificate subject. This certificate was issued to PayPal, so the company's information is displayed at the bottom in the details window. You can also see information that is more useful to applications and computer systems, such as the RSA public key, the object identifiers (OIDs) for the basic and enhanced key usage of the certificate, and so on. Although most users (and even many experienced IT professionals) do not understand all the information in a certificate, it is always available. This availability reflects a core concept of certificates that was explored earlier—namely, that certificates do not contain any data that you do not want to provide to the public. The only data kept secret is the private key (also called the secret key) and it is not part of the certificate.

Note

If we examined the same certificate on the PayPal Web server, it would indicate that there is a stored private key associated with this certificate. Do not misinterpret that the certificate contains the private key. The certificate itself contains only the public key. The private key is stored in the computer but not in the certificate.

Summary

This chapter provides a basic refresher and introduction to PKI and digital certificates. It also defines a number of terms and concepts that we'll be exploring in more detail in later chapters. In addition, we've taken an in-depth look at the contents of certificates and how trust is built from this data. Remember that trust is relative—you might trust certificate *x*, but your peers or family members might not. Trust is made partially of empirical data and partially of personal perception and emotion.

The next chapter will explore how trust is applied when the PKI requires multiple subjects to be trusted, and how that trust can be inefficient if set up incorrectly. We will begin to explore the topic of SAN certificates in some depth and see how they can solve a number of PKI problems with little or no additional investment.

Download Additional eBooks from Realtime Nexus!

Glossary

Most series should have a glossary—including it with Chapter 1 makes it more accessible throughout the series and defines the terms in advance.

Asymmetric Cryptography

A cryptography method where the data is encrypted and decrypted with different keys that are mathematically related; also called public key cryptography.

Certificate

A digitally signed collection of data that asserts and, in some cases, proves an identity.

Certificate Chain

A set of two or more certificates where each certificate trusts another and one certificate (the root certificate) is self-signed.

Certificate Revocation List (CRL)

A collection of certificates that have been revoked by the issuing certification authority (CA).

Certificate Revocation List Distribution Point (CDP)

A location where a CRL is published.

Certification Authority (CA)

A computer that issues certificates to entities and other CAs and vouches for the authenticity of certificates that it issues.

Digital Signature

A combination of a data hash to prove data integrity and public key encryption to prove the identity of the entity vouching for the data; most certificates contain digital signatures.

Hash

A small, unique cryptographic derivative of a message that is often used to prove the authenticity of the message; common hash functions include MD5 and SHA-1.

Issuer

The CA that digitally signs a certificate.

Key

A number that is used in cryptographic functions to encrypt, sign, decrypt, or validate the signature of a message.

Key Usage

A portion of a certificate that specifies which tasks the certificate is authorized to enable.

Message Digest 5 (MD5)

A 128-bit one-way hash function.

Object Identifier (OID)

A long, unique number often used in digital certificates.

Private Key

A cryptographic key that is kept secret and not shared with other parties.

Private Key Cryptography

See symmetric cryptography.

Public Key

A cryptographic key that is not compromised from being well-known to unauthorized parties.

Public Key Cryptography

See asymmetric cryptography.

Public Key Infrastructure (PKI)

A system of clients and certification authorities (CAs) that form a complete trust.

Requestor

The entity that presents a certificate request to an issuing certification authority (CA).

RSA (Algorithm)

A cryptographic algorithm that uses symmetric cryptography to protect and sign data.

Root Certificate

A self-signed certificate at the top of a chain of trust.

Secure Hash Algorithm 1 (SHA-1)

A 160-bit one-way hash function.

Secure Sockets Layer (SSL)

A security protocol that uses asymmetric cryptography to provide authentication, confidentiality, and data integrity; SSL is often used in Web applications.

Symmetric Cryptography

A cryptography method where the data is encrypted and decrypted with the same key; also called private key cryptography.

Trust

A state where a valid certificate is accepted as adequate proof of identity.

Trusted Root

A root certificate that is accepted as trustworthy; when a certificate is presented that chains to a trusted root, that certificate is considered trustworthy.

Validity Period

The time interval during which a certificate is effective.